...o Registro.br

Diretoria de Serviços e de Tecnologia – NIC.br
Frederico A. C. Neves
IX Fórum Regional – 10/06/2019

O que é

Serviço de Registro de **identificadores únicos** para a Internet no Brasil. Operador do **.br** e NIR para o Brasil. Identificadores únicos são fundamentais para a pluralidade e a independência em rede.

- **Domínios**

  *.com.br [DNS / diretório]

  @example.com.br https://www.example.com.br

- **Números**

  ASN *[diretório]*

  64511

  Endereços *[DNS reverso / diretório]*

  IPv4 192.0.2.0/24

  IPv6 2001:DB8::/32

diretório

```
% whois foo53.com.br
...
domain:      foo53.com.br
owner:       Frederico A. C. Neves
ownerid:     151.131.778-73
country:     BR
owner-c:     FAN
admin-c:     FAN
tech-c:      FAN
billing-c:   FAN
nserver:     a.auto.dns.br
nsstat:      20180420 AA
nslastaa:    20180420
nserver:     b.auto.dns.br
nsstat:      20180420 AA
nslastaa:    20180420
dsrecord:    33150 ECDSASHA256 4564B45E49634B8AB183C9823E5B5005F906682D5CD1498094E792D94A800D87
dsstatus:    20180417 DSOK
dslastok:    20180417
created:     20080505 #4428392
changed:     20180425
expires:     20190505
status:      published

nic-hdl-br:  FAN
person:      Frederico Augusto de Carvalho Neves
e-mail:      fneves@registro.br
```

diretório

```
% whois AS22548
…
aut-num:     AS22548
owner:       Núcleo de Inf. e Coord. do Ponto BR - NIC.BR
ownerid:     05.506.560/0001-36
responsible: Demi Getschko
country:     BR
owner-c:     FAN
routing-c:   FAN
abuse-c:     FAN
created:     20011016
changed:     20130306
inetnum:     200.160.0.0/20
inetnum:     2001:12ff::/32
as-in:       from AS3549 100 accept ANY
as-in:       from AS16735 100 accept ANY
as-out:      to AS3549 announce AS22548
as-out:      to AS16735 announce AS22548
```

diretório

```
% whois 200.160.0.0
…
inetnum:     200.160.0.0/20
aut-num:     AS22548
abuse-c:     FAN
owner:       Núcleo de Inf. e Coord. do Ponto BR - NIC.BR
ownerid:     05.506.560/0001-36
responsible: Demi Getschko
country:     BR
owner-c:     FAN
tech-c:      FAN
inetrev:     200.160.0.0/20
nserver:     a.dns.br
nsstat:      20180424 AA
nslastaa:    20180424
nserver:     b.dns.br
nsstat:      20180424 AA
nslastaa:    20180424
nserver:     c.dns.br
nsstat:      20180424 AA
nslastaa:    20180424
```

dns

```
% dig @a.dns.br foo53.com.br a +dnssec +norec +multi

; <<>> DiG 9.12.1 <<>> @a.dns.br foo53.com.br a +dnssec +norec +multi
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57652
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;foo53.com.br. IN A

;; AUTHORITY SECTION:
foo53.com.br.  3600 IN NS a.auto.dns.br.
foo53.com.br.  3600 IN NS b.auto.dns.br.
foo53.com.br.  3600 IN DS 33150 13 2 (
    4564B45E49634B8AB183C9823E5B5005F906682D5CD1
    498094E792D94A800D87 )
foo53.com.br.  3600 IN RRSIG DS 7 3 3600 (20180501100000 20180424100000 4098 com.br.
    YWu8Rebr9WM307/72AXjb+221E3W6lL8OXeaN28Qo6UH
    DFf4V9uBD+wkEoTGA7Kbb4g9jjUM6gf2H10xroW8Okg8
    k04ODbklaTn/THBpyjvHqY8zic0Kz4waaPW+GsggJQio
    x2lV/foi3iIU4HovA2Hr8yKbL4GIxI7+2Bs0pAoJiDWU
    Ra3jeESIWpve7KM2h/PxjLNk0adUb4soj5GaqQ== )
```

Para quem é

- **Domínios**

2,45 milhões de titulares (60/40% pessoas físicas/jurídicas)

4,06 milhões de domínios (90% .com.br, restante distribuído em 120+ DPNs)

76% titulares tem um único domínio

- **Números**

6616 titulares entre Provedores, Empresas, Governo e Universidades

6868 ASNs com 16486 alocações diretas e 150767 sub-designações

Representamos 68% dos ASNs, 60% do IPv4 e 72% do IPv6 atualmente alocado na América Latina

Como atende

Com a divisão em sete gerências com uma equipe especializada de 87 funcionários

- Atendimento
  - 43 funcionários
  - Responsável por uma média de 4000 atendimentos diários (email/telefone)
  - Análise e execução de 2500 procedimentos administrativos por mês
  - Análise e tratamento de 700 procedimentos de revisão administrativa de abusos por mês

Como atende

- Recursos de Numeração
  - 4 funcionários
  - Alocação direta média de 100 novos ASNs/Blocos por mês
  - Monitoração e Tratamento de abusos
  - Monitoração do processo de políticas
- Produtos e Mercado
  - 3 funcionários
  - Análise de mercado e planejamento de novos produtos
  - Atendimento a interface do atacado EPP – 108 provedores
  - Acompanhamento dos processos de liberação competitivos
  - Atendimento aos clientes e acompanhamento de políticas e regulação de gTLDs

Como atende

- Engenharia
  - 9 funcionários
  - Pesquisa e Desenvolvimento de software
  - Sistema de Registro, faturamento, cobrança, provisionamento DNS, diretório whois/rdap, EPP, LACNIC registro e EPP, entre outros
- Sistemas
  - 8 funcionários
  - Administração da Rede / Sistemas / Virtualização / Storage
  - Redes Anycast DNS
    - relacionamento parceiros
  - Suporte TI local / eventos

Como atende

- Infraestrutura
  - 9 funcionários
  - Concepção e Projetos
  - PMOC - 2 instalações críticas NIC-NU / NIC-JD
    - Energia / AC / Incêndio
  - Rede óptica
- Operação - NOC
  - 10 funcionários
  - Monitoração 7x24
    - Infraestrutura Serviços / Rede / Rede Anycast
    - Infraestrutura física
    - Rede do IX
  - Média de 1700 ligações (84% IX) e 500 tarefas concluídas por mês
    - Suporte primeiro nível MEU.IX média 750 interações mês (filas: Suporte, NOC, PREFIXO, PAG, FIBRA).
  - Suporte e administração dos DC
    - Acompanhamento de clientes
      - Negociação / Visitação
      - Controle de chamados
    - Acompanhamento prestadores de serviço
    - Controle físico e de Interconexões

Com o quê atende

- Infraestrutura física
  - 3 Centros de Dados – NIC-JD NIC-NU NIC-FZ
    - NIC-JD – São Paulo
      - Dedicada / Estado da Arte
      - Redundância TIER-IV Elétrica/AC
      - 2.5 MVA instalado
      - 180 racks / 900 kW TI
    - NIC-NU – São Paulo
      - Condomínio
      - 30 racks / 80 kW TI
    - NIC-FZ – Fortaleza
      - DC Comecial
      - 5 racks / 25 kW TI / Jaula
  - Rede Óptica
    - Anel óptico enterrado entre NIC-JD e NIC-NU
    - Duto PEAD 110 mm
    - 20 km, 12km rota A com a prefeitura e 8km rota B com a EMAE
    - Capacidade de 9 cabos ópticos. Atualmente com um cabo de 144 fibras.

Com o quê atende

- Infraestrutura Rede
  - ASN 22548
  - 65 elementos (roteadores, switchs)
  - 4 provedores de trânsito / 35 clientes de trânsito
- Infraestrutura computacional
  - 104 servidores físicos
  - 159 servidores virtuais
  - Storage distribuído
    - 211 TB líquidos
  - 34 servidores de parceiros
    - 17 LACNIC

Com o quê atende

- Rede Anycast
  - 6 ASN com clusters globais
    - 80 servidores DNS sendo 30 anycasts
  - 5 bilhões de respostas/dia - Picos/média de 80/60 kqps
  - Capacidade instalada distribuída
    - 2 ordens de grandeza

      maior que o tráfego regular

com.br - 690µs									
		1	2	3	4	5	6	7	8
a	398µs	387µs	399µs	384µs	429µs	431µs	379µs	383µs	416µs
b	496µs	8	8	9	8		9		
c	479µs	32	33	33	37	32	37	37	37
d	584µs	178	178	178	178	178	178	178	178
e	538µs	198	198	198	198	198	197	198	198
f	552µs	312	300	300	300	312	300		
z		411µs	405µs	400µs	409µs	401µs	389µs	424µs	396µs
ba		17	17	34	201	357	251	291µs	
ca		4	18	3	242	30	276µs		
da		402µs	7	8	17	39	238		
ea		434µs	16	33	46	81			
fa		414µs	8	7	78	213	50		

OK	SOAVer	Timeout	Other	NXDomain

default: ms

Com quem colabora

- +40 instituições correlatas, de pesquisa, prestação de serviços ou de desenvolvimento de protocolos.
- Brasil
  - RNP USP UNESP UFRGS UFPR UFMG UFSC UFBA
  - IMA ETICE Embratel
  - ON STF
- +20 instituições internacionais com a troca de infra-estrutura computacional ou prestação de serviços recíprocos.
  - DENIC KRNIC
  - NIC.LV NIC.RU NIC.AT NIC.GR APNIC ICANN ISC NETNOD
  - NIC.AR CIRA SWITCH NIC.CL NIC.PE
  - NIC.PY NIC.BO NIC.SV SeCIU NIC.GH NIC.PA NIC.PT CENIAInternet NIC.GT
- IETF OARC LACNIC NLNETLabs

Melhorando

- Inovação no sistema de publicação DNS
  - Agilidade Criptográfica
  - Migração para ECDSA
  - Redução no intervalo de publicação
    - de 30’ para 5’
- Mudanças em procedimentos Administrativos
  - Transferência de titularidade
  - Cancelamento

Melhorando

- Nova interface para sistema de IPs
  - DNSSEC p/ reverso
  - Preparação RPKI
  - Investimento em Software Livre
    - RPKI Tools – NLNetLabs
- Autenticação FIDO2
  - Segundo Fator E2E
  - WebAuthN

Obrigado!

Comentários / Perguntas?

Motivação para o Alg. Roll

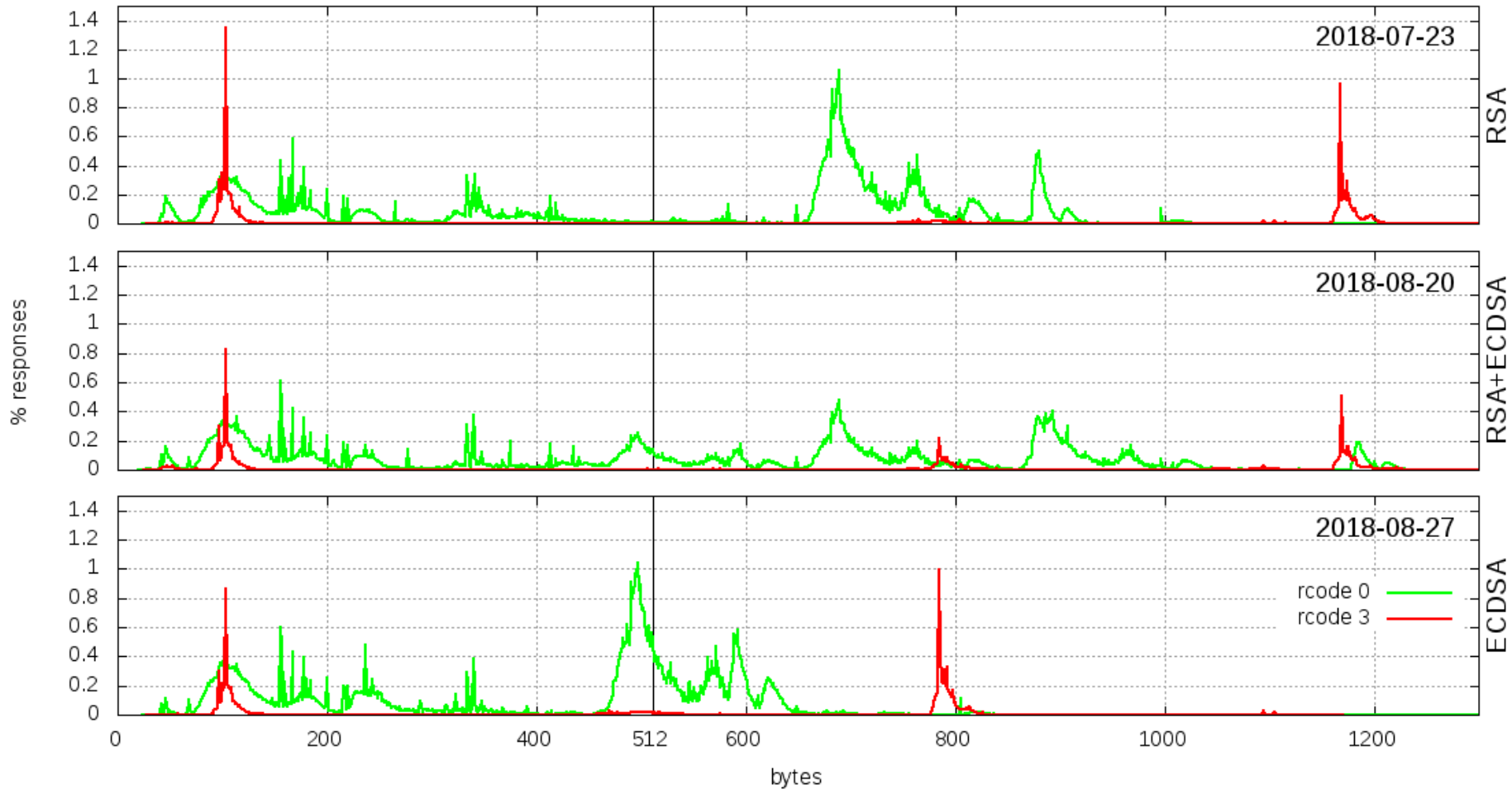
Agilidade Criptográfica - Estar preparado para uma troca de algoritmo criptográfico. Exercitar esta troca fora de uma situação de emergência.

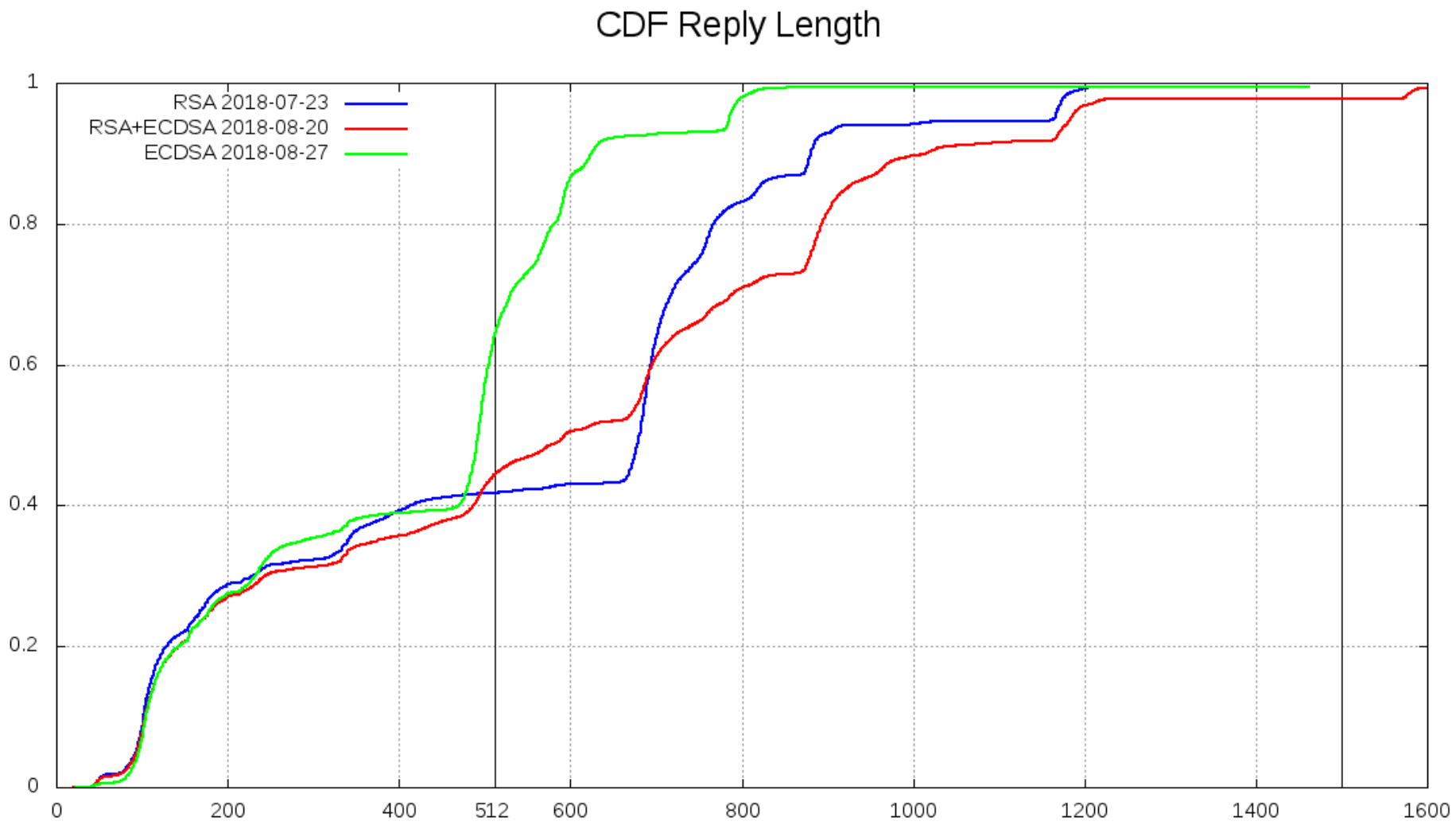
Atualização Criptográfica – Ainda estamos usando RSA/SHA1 desde 2007. ECDSAP256SHA256 prove segurança muito maior do que RSA de tamanho equivalente. Para um mesmo nível de segurança (128 bits simétricos) seria necessário uma chave 6 vezes maior (3072 bits)

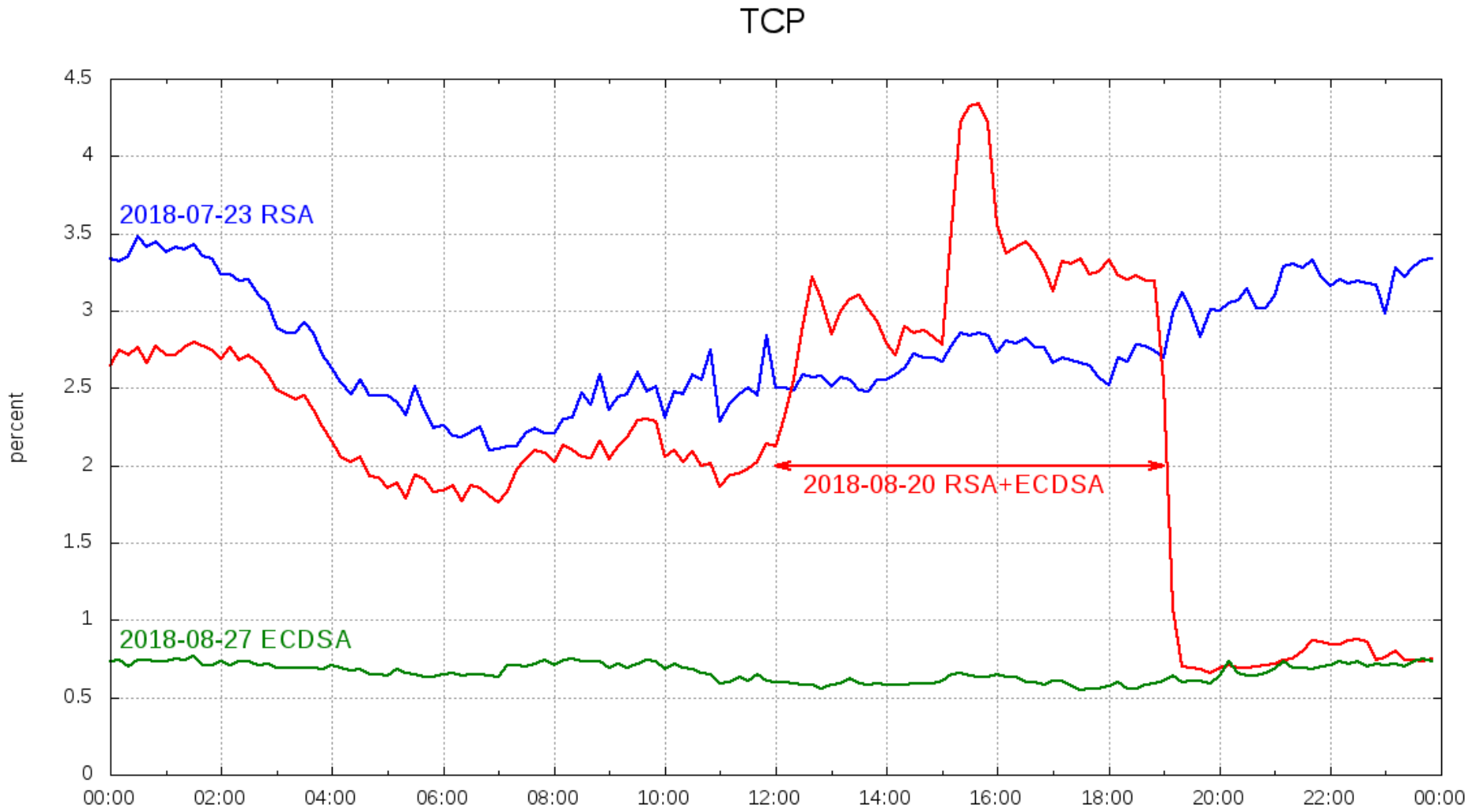
Reduzir substancialmente o tamanho da zona e das respostas DNS com a adoção de curva eliptica – ECDSAP256SHA256. A ZSK/CSK hoje tem 1280 bits com o novo algoritmo terão somente 512 bits. Uma redução de 60% no tamanho das assinaturas nas respostas DNS. A grande maioria das respostas ficará abaixo de 512 bytes.

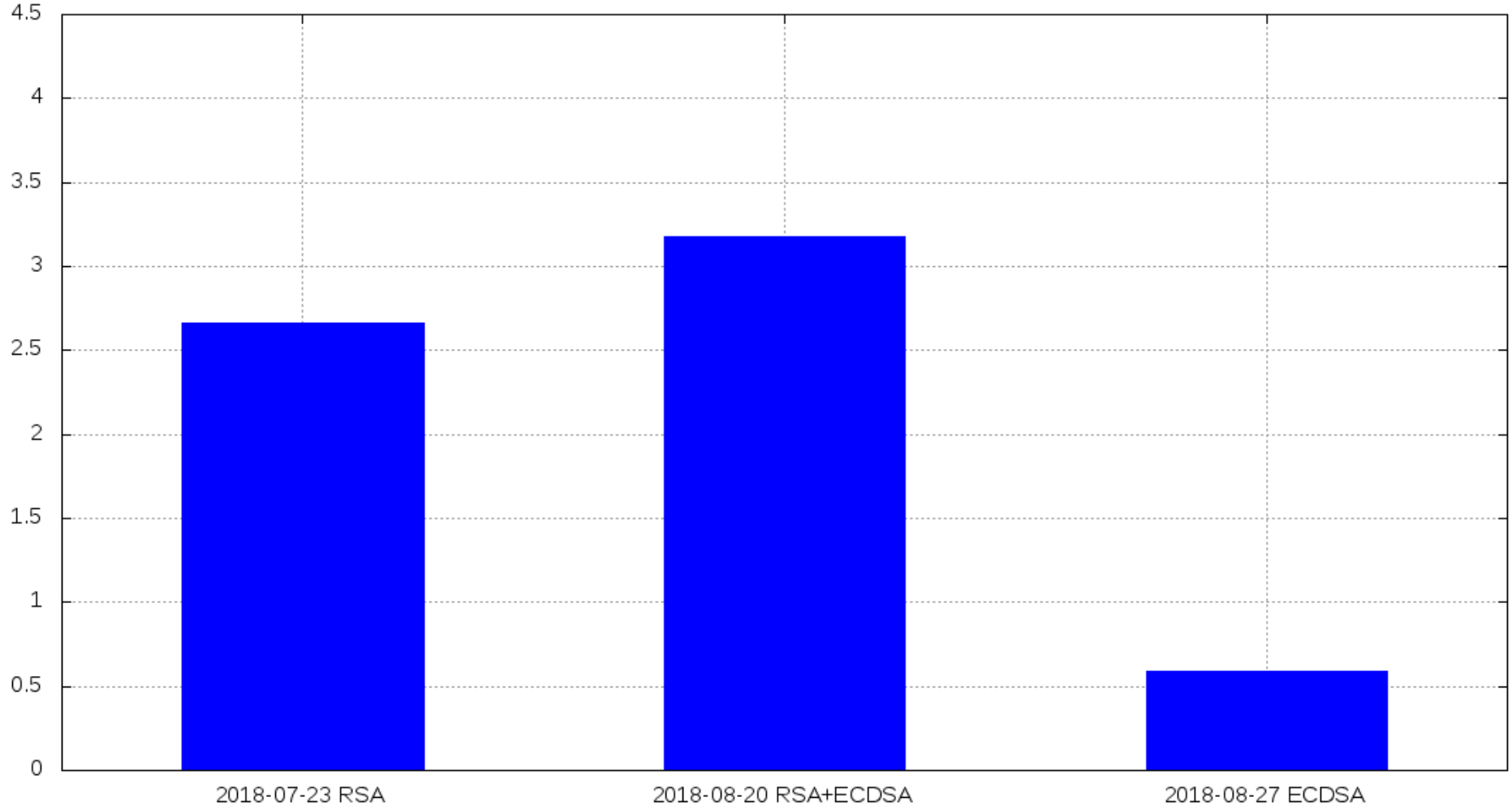
ECDSAP256 é um passo intermediario para o objetivo de adotar as novas curvas propostas pelo IETF RFCs 8032/7738 nos próximos 5 anos - ED25519 alg. 15.

Reply Length




CDF Reply Length
RSA 2018-07-23
RSA+ECDSA 2018-08-20
ECDSA 2018-08-27
1
0.8
0.6
0.4
0.2
0
0
200
400
512
600
800
1000
1200
1400
1600


TCP
percent
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
2018-07-23 RSA
2018-08-20 RSA+ECDSA
2018-08-27 ECDSA


4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
2018-07-23 RSA
2018-08-20 RSA+ECDSA
2018-08-27 ECDSA